

Slide 1 of 30



## Today's Topics • Background - Commonwealth Context - Work Group events to date • About Digital Signatures

2

Slide 2 of 30

Key Findings & Recommendations

Discussion











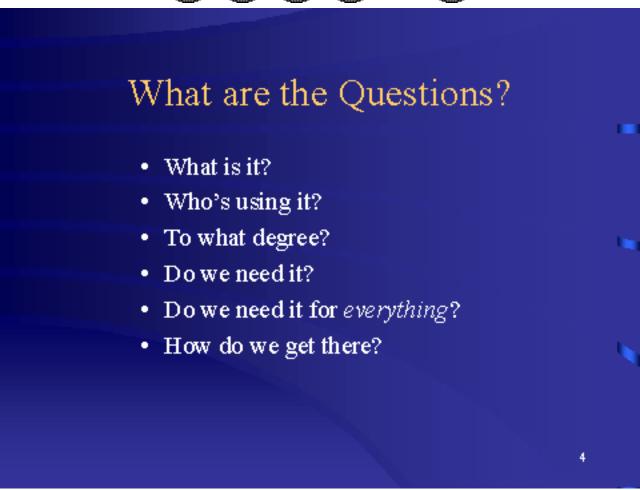
#### Work Group Events since June

- · Monthly PSA Work Group sessions
- · Presentation for COTS
- Panel at COVITS (Health Canada, Federal PKI Steering Committee & Capital One)
- · Monitoring legislative developments
  - Federal, state & model
- Video teleconference with the State of Washington
- Planning "First Wave" agencies at DGIF
- Federal Bridge Certification Architecture at UVa

3

Slide 3 of 30





Slide 4 of 30



# What a Digital Signature is NOT • NOT a handwritten signature • NOT a digitized signature • NOT the same as an electronic signature

5

Slide 5 of 30



#### What a Digital Signature IS

- It results from an arithmetic operation on data
  - the data it "signs" cannot be altered without detection
- It uses public & private "keys"
- It relies on "certificates" issued to individuals within a PKI
- It involves sophisticated encryption
- · It provides
  - a high level of authentication
  - technical non-repudiation
  - confidentiality

6

Slide 6 of 30



#### Demystifying Digital Signatures

A video, courtesy of Washington State
 Department of Information Services

7

Slide 7 of 30



#### "Electronic" or "Digital"

- "Digital" is a subset of "electronic"
- There are a variety of ways to create an 'electronic' sig:
  - -PIN's
  - digitized (stroked) signatures
  - other forms of biometrics
  - or even double-clicks
  - .... any electronic form, given with the "intent to sign"

8

Slide 8 of 30











## Are Digital Certificates & signatures "right" for every signing process?

- Not necessarily a spectrum of electronic signatures could be valid
- A variety of electronic signatures are already in use (e.g., digitized signatures on the Driver's license, PIN numbers, etc.)
- Criteria should be applied appropriately to match methods of e-signing to business processes

9

Slide 9 of 30



#### Parts of a "managed" PKI?

- Key "PKI" components include
  - Registration Authorities authenticate individual id's
  - Certification Authorities vouch for validity of certificates
  - Certificate Repositories publicly available databases
  - Mechanism to recover/reissue lost/compromised keys
  - Certificate Policies & other governing practices

10

Slide 10 of 30



#### What is a "PKI"

- A "public key infrastructure" is the complex framework within which digital signatures operate
  - to associate individuals reliably with the public key of a public/private key pair
- PKI = laws, policies, hardware, software, business processes & people

11

Slide 11 of 30





#### Other Key Points about PKI's

- 1 The technology works -- we don't need to prove it
- 2 Standards are still evolving but well developed enough to proceed
- 3 The technology is new & complex, BUT the hardest issues to resolve will be policy, legal, and business
- 4 A PKI is costly.... but compared to what?

12

Slide 12 of 30









## What are the trends toward adoption?

- · To this point, relatively slow
- · Pace will quicken
- Demand will grow
- The number & pace of pilots, deployments & legislative initiatives is growing
  - nationally & internationally

13

Slide 13 of 30









#### Growth in Federal Certificates in 2000

- FAA from 1000 to 20,000
- FDIC from 1000 to 7,000
- NASA from 1000 to 25,000
- DOE from 1000 to 20,000
- DOD has issued 50,000 certificates
  - By 2002, 4 Million

14

Slide 14 of 30



#### Progress in Other States

- A number of states have limited deployments running as pilots or production
- A number of others have active RFP's outstanding
  - including Washington, Illinois, Texas & New York
  - California and Minnesota are also active

15

Slide 15 of 30



#### Our current position.....

We are well behind the feds

We are behind a number of other states,
but not at the back of pack

We can gain a leadership position by

- leveraging the experiences of other states
- adapting "best of breed" or model policies and practices to Virginia's needs

16

Slide 16 of 30



## Does COVA need a PKI & Digital Signatures?

- Yes
- Digital signatures are a key element of a robust e-commerce environment
- · Failure to provide will
  - impede e-commerce and economic growth
  - postpone realizing the associated benefits of convenience and efficiency

17

Slide 17 of 30



#### 1. Decide & Commit NOW

- To keep pace with outside events
- To be ready for the 2001 General Assembly work needs to be completed before this time next year
- Work must begin today

18

Slide 18 of 30



#### 2. Proposals for the 2000 General Assembly

- Proposed legislation
  - to <u>retain</u> ability to adopt digital signatures, and
  - to <u>restore</u> ability to adopt *other* forms of electronic signatures
- A resolution supporting policies & principles

19

Slide 19 of 30



### 3. Develop Bridge Certification Architecture

- · Based on the federal model
- In collaboration with First Wave efforts
- University of Virginia to lead

20

Slide 20 of 30



## 4. Commission *First Wave*Deployments

First Wave will demonstrate:

- Internal to an agency
- · Agency to agency
- Agency to business partners
- Agency to local government
- Agency to general public (limited client population)

21

Slide 21 of 30



#### First Wave Sponsors

- Agencies & Localities
  - Chesterfield County
  - Department of Game & Inland Fisheries
  - Department of Information Technology
  - Department of Motor Vehicles
  - Department of Transportation
  - Fairfax County
  - VIPNet
- Others may join by proposal within 30 days.

22

Slide 22 of 30



#### Oversight, Coordination & Staffing

- · Appoint an Oversight Committee
  - Chaired by Secretary of Technology
- Establish a new COTS work group
  - Assisted by full time staff
  - Including appointed central agency participants
  - Including industry partners
  - In collaboration with CBCA initiative
  - PSA Work Group addresses broader, ongoing agenda

23

Slide 23 of 30



#### 6. Interim Certificate Authorities

- Department of Game & Inland Fisheries
- VIPNet contractor in agreement with the Department of Information Technology
- Any others -- tbd

24

Slide 24 of 30



#### 7. Funding

- · Short term
  - Up to \$100k from the Technology Infrastructure Fund
  - First Wave organizations
- Longer term
  - Appropriations

25

Slide 25 of 30



## The Seven Point Plan, in summary.....

- 1 Decide and commit
- 2 Pursue support in the 2000 General Assembly
- 3 **Develop a COVA** Bridge Certification Architecture
- 4 Commission First Wave Deployments
- 5 Establish project Oversight & Plans
- 6 Designate interim Certificate Authorities
- 7 Provide Seed Money

26

Slide 26 of 30



#### Results of the Plan

- > Foundation of operating decisions & rules
- > A Bridge Certification Architecture
- > An Enterprise PKI Architecture
- > An Acquisition Strategy
- > Business Model
- Invested knowledge & skills base
- Trust & confidence in a working solution, extensible to other Commonwealth public sector, business partners & to the public

27

Slide 27 of 30



# What about.... Biometrics? Smart cards? VPN's? S/mime and other standards? Interfacing with legacies? Single sign on?

28

Slide 28 of 30

· Interoperability?



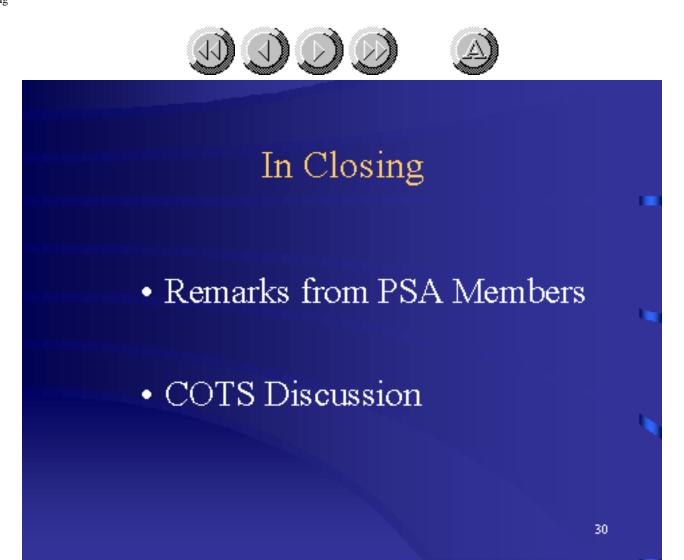
#### A Final Report.....

#### A Work in Progress

- · Many important questions remain
- Some are within our influence & control
  - · our own legal, policy & business frameworks
  - · products, tools, architectures & standards
  - pace
- Some are being driven by external events
  - · federal legislation
  - · evolution of standards
  - · evolution of products & tools

29

Slide 29 of 30



Slide 30 of 30